AMENDMENTS TO THE CLAIMS

Applicants submit below a complete listing of the current claims, including marked-up claims with insertions indicated by underlining and deletions indicated by strikeouts and/or double bracketing. This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of the Claims

1. (Previously presented) A computer-implemented method, comprising:

receiving, by an operating system and/or an enforcement module which is associated with or is part of the operating system, a call from [[an]] a firewall aware application via a first application programming interface, the call having parameters for a connection to an endpoint that the firewall aware application desires to establish, whereby the firewall aware application explicitly communicates a request to traverse a firewall to establish the connection, the request is being directed to a specific socket and includes handling requirements for data sent and/or received by the firewall aware application; and

making, by the operating system and/or the enforcement module, a call via a second application programming interface to the firewall to establish the connection in accordance with the parameters.

2. (Original) The method of claim 1, further comprising, at the firewall, evaluating the parameters with respect to a policy and, if the parameters meet the policy, establishing the network connection in accordance with the parameters.

3. (Original) The method of claim 1, wherein the parameters comprise a known endpoint to which the application would like to be connected.

4. (Original) The method of claim 3, wherein the parameters further comprise a request to limit the connection to a single connection.

5. (Original) The method of claim 4, further comprising, after the connection has been established, closing the connection in accordance with the request.

6. (Previously presented) The method of claim 1, wherein the parameters comprise a request for bandwidth or connection throttling for the connection.

7. (Original) The method of claim 1, wherein the parameters comprise limiting the connection to a subset of interfaces, local addresses, or remote addresses, or combinations thereof.

8. (Original) The method of claim 1, wherein the parameters comprise a timeout policy for the connection.

9. (Original) The method of claim 1, wherein the parameters comprise turning off or on specific protocol options.

10. (Original) The method of claim 1, wherein the parameters comprise information about a property of a flow that requires special handling.

11. (Original) The method of claim 10, wherein the information comprises a request for authentication or encryption.

12. (Previously presented) The method of claim 1, wherein the application explicitly communicates the request to establish the connection by opening a listening socket.

13. (Previously presented) The method of claim 1, wherein the application explicitly communicates the request to establish the connection by connecting to a socket.

14. (Original) The method of claim 1, wherein the call to the firewall is made via a firewall application programming interface.

15. (Original) The method of claim 1, wherein the firewall is located on a computer with the application.

16. (Original) The method of claim 1, wherein the firewall comprises an edge firewall, and further comprising an agent to communicate information to the edge firewall about the connection.

17. (Original) The method of claim 1, wherein the firewall comprises an edge firewall, and further comprising an authenticated protocol to communicate information to the edge firewall about the connection.

18. (Previously presented) A computer-storage medium encoded with a computer program for performing the method recited in claim 1.

19. (Currently amended) A computer system comprising:

an operating system;

a first application programming interface associated with the operating system and configured and adapted to receive a call from [[an]] a firewall aware application, the call having parameters for a connection to an endpoint that the firewall aware application desires to establish, whereby the firewall aware application explicitly communicates a request to traverse a firewall to establish the connection, the request is being directed to a specific socket and includes handling requirements for data sent and/or received by the firewall aware application; and

an enforcement module associated with or is part of the operating system and called via the application programming interface and configured and adapted to:

receive an indication from the application that the application desires to establish the connection; and make a call via a second application programming interface to a firewall to establish the connection in accordance with the parameters.

20. (Original) The computer system of claim 19, further comprising a firewall application programming interface for making the call to the firewall.

21. (Currently amended) A computer-implemented method, comprising:

receiving, by an interception module communicating with a firewall via a first application programming interface~~ and including~~, via a second application programming interface at least one policy established by a first user that permits ~~for~~ at least one of ~~the user,~~ an application and a service to connect to a network when the first user runs the at least one of the application and a service, wherein the at least one policy is stored among a plurality of policies in a policy cache of the interception module;

~~to establish at least one policy from a plurality of policies stored in a policy cache of the interception module, and a filter cache,~~

receiving, by the interception module a connect attempt, a listen attempt, or a combination thereof from [[an]] the application or [[an]] the service run by a second user;

extracting, by the interception module, user and application or service information from the connect attempt, the listen attempt, or the combination thereof;

~~identifying~~ determining, by the interception module, an identity of the second user and [[the]] what application or [[the]] what service is making the connect attempt, the listen attempt, or the combination thereof~~ from the user and application or service information~~;

determining ~~evaluating~~, by the interception module, whether the identity of the second user matches an identity of a user that established the at least one policy and whether ~~the application or service information to determine if~~ the connect attempt, the listen attempt, or the combination thereof comply with the at least one policy~~ one or more policies from the plurality of policies~~; and

[[if]] when the connect attempt, the listen attempt, or the combination thereof comply with the at least one policy and the identity of the second user matches the identity of the user that established the at least one policy ~~one or more policies from the plurality of policies~~, instructing, by the interception module, the firewall to automatically create a configuration to allow the connect attempt, the listen attempt, or the combination thereof, and storing the configuration in [[the]] a filter cache of the interception module.

22. (Currently amended) The method of claim 21, further comprising sending a notification to a user of [[if the]] a connect attempt, [[the]] a listen attempt, or [[the]] a combination thereof~~ do not comply with one or more policies from the plurality of policies, sending a notification to the user of the application or service~~.

23. (Currently amended) The method of claim 22, wherein sending the notification comprises receiving a user input indicative of ~~selection to~~ allowing a connection thereby creating the at least one policy.

24. (Currently amended) The method of claim 21, wherein establishing the at least one policy further comprises receiving a policy from the application or service.

25. (Currently amended) The method of claim 24, wherein receiving the policy comprises receiving the policy via [[the]] an application programming interface.

26. (Currently amended) The method of claim 24, wherein the policy received from the application or service comprises inbound or outbound restrictions using one or more of Internet Protocol addresses, information about a subnet, information about scope of the connection, or combinations thereof.

27. (Original) The method of claim 24, wherein the policy received from the application or service comprises communication security level.

28. (Original) The method of claim 27, wherein the communication security level comprises authentication.

29. (Original) The method of claim 27, wherein the communication security level comprises encryption.

30. (Currently amended) The method of claim 21, wherein the firewall comprises a host firewall located on a computer comprising ~~with~~ the application or the service.

31. (Original) The method of claim 21, wherein the firewall comprises an edge firewall, and further comprising an agent to communicate information about the connection.

32. (Original) The method of claim 21, wherein the firewall comprises an edge firewall, and further comprising an authenticated protocol to communicate information to the edge firewall about the connection.

33. (Previously presented) A computer-storage medium encoded with a computer program for performing the method recited in claim 21.

34-36. (Canceled)

37. (Currently amended) A computer system, comprising:

a firewall; and

an interception module communicating with the firewall via a first application programming interface, the interception module including a second application programming interface for establishing, by a first user, at least one policy that permits at least one of ~~at least one of a user,~~ an application and a service to connect to a network when the first user runs the at least one of the application and a service~~to establish at least one policy from a plurality of policies~~, wherein the at least one policy is stored in a policy cache of the interception module~~, and a filter cache and~~, the interception module is configured and adapted to:

intercept a request for a connect attempt, a listen attempt, or a combination thereof from the application or the service run by a second user;

extract user and application or service information from the connect attempt, the listen attempt, or the combination thereof;

identify the user and the application or the service from the user and application or service information;

~~evaluate~~ determine whether an identity of the second user matches an identity of a user that established the at least one policy and whether ~~the application or service information to determine if~~ the connect attempt, the listen attempt, or the combination thereof comply with the at least one policy ~~one or more policies from the plurality of policies~~; and

[[if]] when the connect attempt, the listen attempt, or the combination thereof comply with the at least one policy and the identity of the second user matches the identity of the user that established the at least one policy, instructing the firewall to create a configuration to allow the connect attempt, the listen attempt, or the combination thereof, and storing the configuration in [[the]] a filter cache of the interception module.

38. (Canceled)

39. (Previously presented) The computer system of claim 37, wherein the interception module comprises a firewall client for communicating information about the connect attempt, the listen attempt, or the combination thereof to an edge firewall.